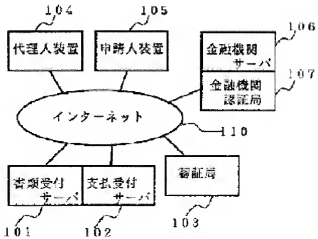
SYSTEM FOR SENDING DOCUMENT AND METHOD THEREFOR

Publication number: JP11175607
Publication date: 1999-07-02
Inventor: HIROTA JUNKO; TAKEUCHI SATOSHI; YAMABE KOICHI
Applicant: HITACHI LTD
Classification:
- international: ***G06Q50/00; G06Q10/00; G06Q20/00; G07F17/16;*** **G06Q50/00; G06Q10/00; G06Q20/00; G07F17/00;** (IPC1-7): G06F17/60
- European: G07F17/16
Application number: JP19970352243 19971205
Priority number(s): JP19970352243 19971205

Also published as:
E P0921484 (A2)
US 6868402 (B1)
E P0921484 (A3)
CN16 04095 (A)
CN14 97482 (A)
more >>

Abstract of **JP11175607**

PROBLEM TO BE SOLVED: To properly attain electronic document sending and charge payment through communications without preparing any special account such as preliminary deposit account by connecting a payment accepting server with a network, and requesting charge payment to the payment accepting server by an applicant device. SOLUTION: An applicant is connected from an applicant device 105 with a payment accepting serve 102, and a charge payment processing is operated. The payment accepting server 102 is connected with a financial institution server 106, and the collation of the credit of the applicant is executed, and a payment certificate is transmitted to the applicant device 105. The applicant adds a payment certificate to document data, and transmits it to a substitute device 104. A substitute receives data by the substitute device 104, and temporarily preserves the data. In an arbitrary period, the substitute transmits the data to a document accepting server 101. The document accepting server 101 receives the data (data obtained by adding the payment certificate to the document data), verifies the payment certificate, and preserves the document data.



(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（Ａ）　(11)特許出願公開番号

特開平11－175607

(43)公開日　平成11年(1999) 7月2日

(51)Int.Cl.[6]　識別記号　ＦＩ

Ｇ０６Ｆ　17/60　Ｇ０６Ｆ　15/21　Ｚ

審査請求　未請求　請求項の数６　ＦＤ　（全 20 頁）

(21)出願番号　特願平9－352243

(22)出願日　平成９年(1997)12月５日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　廣田　純子
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　武内　敏
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(72)発明者　山部　浩一
神奈川県横浜市戸塚区戸塚町5030番地　株式会社日立製作所ソフトウェア開発本部内

(74)代理人　弁理士　矢島　保夫

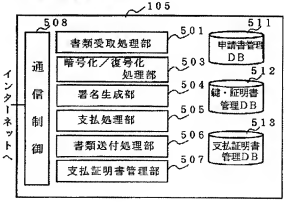
(54)【発明の名称】　書類送付システムおよび方法

(57)【要約】

【課題】インターネットなどを介して通信で電子的な書類提出を行なう際に手数料の支払いが必要な場合において、予納口座のような特別な口座を作る必要が無く、クレジットカードや銀行口座から別フェーズで引き落とし処理を行なうことも無く、また料金を支払う者と書類の提出を行なう者とが異なる場合でも適正に書類提出とその料金支払いを行なうことができる書類送付システムおよび方法を提供することを目的とする。また、通信で電子的な書類提出を行なう場合に、悪用を許すことなく、提出日時を合理的に決定する仕組みを備えた書類送付システムおよび方法を提供することを目的とする。

【解決手段】ネットワーク上に支払い受付サーバを設け、該支払い受付サーバに対して支払い依頼を出せば、支払い受付サーバが信用照会を実施し、料金の支払いが保証される場合にはその旨を示す改ざん不可能な形式の支払い証明書を発行するようにする。書類を提出する際には、この支払い証明書を付して送信する。

申請人装置の構成



1

【特許請求の範囲】

【請求項１】ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、

前記ネットワークに、支払い受付サーバを接続し、

前記申請人装置は、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼する手段を備え、

前記支払い受付サーバは、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信する手段とを備え、

前記申請人装置は、送付する書類に前記支払い証明書を付して改ざん不可能な形式である支払い証明書付き書類とし、前記書類受付サーバに送信する手段を備え、

前記書類受付サーバは、前記申請人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管する手段を備えたことを特徴とする書類送付システム。

【請求項２】ネットワーク経由で、申請人装置が送付したい書類を、代理人装置が代理して書類受付サーバに対して送付する書類送付システムにおいて、

前記ネットワークに、支払い受付サーバを接続し、

前記申請人装置は、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼する手段を備え、

前記支払い受付サーバは、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信する手段とを備え、

前記代理人装置は、受信した支払い証明書付き書類を前記書類受付サーバに送信する手段を備え、

前記書類受付サーバは、前記代理人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管する手段を備えたことを特徴とする書類送付システム。

【請求項３】ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、該書類の送付に伴う料金の支払いを受付ける支払い受付サーバであって、

前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、

該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信する手段とを備えたことを特徴とする書類送付システムの支払い受付サーバ。

2

【請求項４】ネットワーク経由で、所定の装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、

前記書類を送付する装置で、送付したい書類データに一方向関数を施して圧縮データを取得し、該圧縮データを改ざん不可能な形式で前記書類受付サーバに送信する手段と、

前記書類受付サーバで、受信した圧縮データを記憶したのち、前記書類を送付する装置にチケットを送信する手段と、

前記書類を送付する装置で、チケットを受信したら、送付したい書類データの前記書類受付サーバへの送信を実行する手段と、

前記書類受付サーバで、前記書類データをすべて受信したら、該書類データに前記一方向関数を施して得た圧縮データと、前記記憶してある圧縮データとを比較し、それらの圧縮データが一致することを確認する手段とを備えたことを特徴とする書類送付システム。

【請求項５】ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付方法において、

前記ネットワークに、支払い受付サーバを接続するとともに、

前記申請人装置から、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼するステップと、

前記支払い受付サーバにより、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施するステップと、

該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信するステップと、

前記申請人装置により、送付すべき書類に前記支払い証明書を付して改ざん不可能な形式である支払い証明書付き書類とし、前記書類受付サーバに送信するステップと、

前記書類受付サーバにより、前記申請人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管するステップとを備えたことを特徴とする書類送付方法。

【請求項６】ネットワーク経由で、所定の装置から書類受付サーバに対して書類を送付する書類送付方法において、

前記書類を送付する装置で、送付したい書類データに一方向関数を施して圧縮データを取得し、該圧縮データを改ざん不可能な形式で前記書類受付サーバに送信するステップと、

前記書類受付サーバで、受信した圧縮データを記憶したのち、前記書類を送付する装置にチケットを送信するステップと、

前記書類を送付する装置で、チケットを受信したら、送付したい書類データの前記書類受付サーバへの送信を実行するステップと、

前記書類受付サーバで、前記書類データをすべて受信したら、該書類データに前記一方向関数を施して得た圧縮データと、前記記憶してある圧縮データとを比較し、それらの圧縮データが一致することを確認するステップとを備えたことを特徴とする書類送付方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、電子データで各種の書類を送付・受付し、該書類の送付・受付に伴う料金の支払いやその支払い受付を行なう書類送付システムおよび方法に関する。

【０００２】

【従来の技術】近年、インターネットのようなオープンなネットワーク環境において、各種の書類データの授受や商取引が行なわれるようになってきており、将来的にもさらに多種多様な形態になることが予測される。例えば、現在、特許庁への出願書類などの提出は、提出者が、直接、ダイヤルアップで特許庁のサーバに接続し提出書類データを送信することが可能になっているが、将来的にはインターネット経由で接続することが考えられる。一方、不動産登記や商業登記など、あるいは役所での住民票その他の証明書の発行業務などでは、申請する者が登記所や役所に直接出向いて書類（各種申請書）を提出して手続する必要があるが、このような業務も将来的にはインターネット経由で実施できるようになることが考えられる。

【０００３】このようにインターネットなどを介して通信で電子的な書類提出を行なう場合、その書類提出に伴って手数料の支払いが必要なことがある。特許庁、登記所、あるいは役所などの官公庁に対して提出する書類では、印紙や証紙などを購入しそれを提出書類に貼付して提出する形態をとることが多いが、通信で書類提出を行なう場合には何らかの手数料支払いの仕組みが必要となる。特許庁の電子出願システムでは、あらかじめ書類提出者が予納口座に幾らかの金額を振込んでおき、特許庁の側のシステムでは出願を受け付けたときに当該予納口座から必要な金額を引き落とす形態を採る。

【０００４】一方、いわゆる電子ショッピングなどと呼ばれている商取引では、インターネット経由で種々の商品を購入できるが、その支払いは、通常、クレジットカードや銀行口座からの引き落としで行なわれている。具体的には、商品を購入する者が、通信でクレジットカードや銀行口座の番号を送信し、商品を売る側ではその番号によってクレジットカードや銀行口座から所定の金額を引き落とす。また、近年ではＳＥＴ（Secure Electoronic Transaction）と呼ばれるインターネットの電子決済方式なども提案されている。

【０００５】

【発明が解決しようとする課題】上述したようにインターネットなどを介して通信で電子的な書類提出を行なう際に手数料の支払いが必要な場合、特許庁の電子出願システムのような予納口座からの引き落としの方式では、書類提出を行なう者が必ず予納口座を作らなければならず不便である。不動産登記などの申請では、その書類提出を行なう者が生涯に１度しかその手続を行なわないことも考えられるので、そのためだけに予納口座を作るのは面倒である。

【０００６】予納口座によらない支払方法としては、クレジットカードや銀行口座からの引き落としがあるが、その場合は、申請者が指定したクレジットカードや銀行口座から引き落とす処理を、通信による書類の提出受付け処理とは別フェーズで行なわなければならない。したがって、例えば口座に預金されている金額が引き落とし金額に満たないために引き落としができなくなるケースなどがある。

【０００７】上述のＳＥＴのプロトコルによればインターネット上で電子決済できるが、これは商品を購入する者とその代金を支払う者が同じ者であって、商品購入の申込時に同時に決済を行なうことを前提としており、特許庁、登記所、あるいは役所などの官公庁に対して印紙や証紙などを貼付して書類を提出する形態の手続に適用するにはなじまない。そのような手続では、書類の申請者の代理人が申請者を代行して書類送付を行なう場合があるからである。すなわち、書類に添付する証紙や印紙などは書類の申請者が支払うべきものであり、一方、書類は代理人が提出するので、料金を支払う者と書類を提出する者とが異なることになり、その場合、書類の提出手続と関係付けつつＳＥＴのプロトコルで支払い手続を行なうことはできない。料金の支払いと書類の提出とを無関係に行なうのであれば、料金の支払いにＳＥＴのプロトコルを使用できるが、その場合は料金の支払い手続と書類の提出手続との関係付けがなされない。無理に関係付けようとすると、その分の手間がかかってしまう。

【０００８】さらに、各種書類の提出に際して、その提出がいつ行なわれたかの日時を明確に確定することが必要な場合がある。一方、通信で書類提出を行なう場合は、通信回線の状態などに応じて再送が発生することがあり、書類の提出時点は明確でないという不都合がある。特に、書類の送信を開始した時点を書類の提出時点とした場合は、送信を開始して提出日時を確保した後、再送が発生したことを理由に後から別の内容の書類を送信し、その書類が前記提出日時に提出されたと主張するような悪用が可能になってしまう。したがって、通信で書類を提出する際の提出時点を合理的に確定する仕組み

が求められている。

【０００９】本発明は、上述の従来形における問題点に鑑み、インターネットなどを介して通信で電子的な書類提出を行なう際に手数料の支払いが必要な場合において、予納口座のような特別な口座を作る必要が無く、クレジットカードや銀行口座から別フェーズで引き落とし処理を行なうことも無く、また料金を支払う者と書類の提出を行なう者とが異なる場合でも適正に書類提出とその料金支払いを行なうことができる書類送付システムおよび方法を提供することを目的とする。

【００１０】また、本発明は、通信で電子的な書類提出を行なう場合に、悪用を許すことなく、提出日時を合理的に決定する仕組みを備えた書類送付システムおよび方法を提供することを目的とする。

【００１１】

【課題を解決するための手段】上記目的を達成するため、請求項１に係る発明は、ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、前記ネットワークに、支払い受付サーバを接続し、前記申請人装置は、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼する手段を備え、前記支払い受付サーバは、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信する手段とを備え、前記申請人装置は、送付する書類に前記支払い証明書を付して改ざん不可能な形式である支払い証明書付き書類とし、前記書類受付サーバに送信する手段を備え、前記書類受付サーバは、前記申請人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管する手段を備えたことを特徴とする。

【００１２】請求項２に係る発明は、ネットワーク経由で、申請人装置が送付したい書類を、代理人装置が代理して書類受付サーバに対して送付する書類送付システムにおいて、前記ネットワークに、支払い受付サーバを接続し、前記申請人装置は、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼する手段を備え、前記支払い受付サーバは、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信する手段とを備え、前記申請人装置は、送付する書類に前記支払い証明書を付して改ざん不可能な形式である支払い証明書付き書類とし、前記代理人装置に送信する手段を備え、前記代理人装置は、受信した支払い証明書付き書類を前記書類受付サーバに送信する手段を備え、前記書類受付サーバは、前記代理人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管する手段を備えたことを特徴とする。

【００１３】請求項３に係る発明は、ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、該書類の送付に伴う料金の支払いを受付ける支払い受付サーバであって、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施する手段と、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信する手段とを備えたことを特徴とする。

【００１４】請求項４に係る発明は、ネットワーク経由で、所定の装置から書類受付サーバに対して書類を送付する書類送付システムにおいて、前記書類を送付する装置で、送付したい書類データに一方向関数を施して圧縮データを取得し、該圧縮データを改ざん不可能な形式で前記書類受付サーバに送信する手段と、前記書類受付サーバで、受信した圧縮データを記憶したのち、前記書類を送付する装置にチケットを送信する手段と、前記書類を送付する装置で、チケットを受信したら、送付したい書類データの前記書類受付サーバへの送信を実行する手段と、前記書類受付サーバで、前記書類データをすべて受信したら、該書類データに前記一方向関数を施して得た圧縮データと、前記記憶してある圧縮データとを比較し、それらの圧縮データが一致することを確認する手段とを備えたことを特徴とする。

【００１５】請求項５に係る発明は、ネットワーク経由で、申請人装置から書類受付サーバに対して書類を送付する書類送付方法において、前記ネットワークに、支払い受付サーバを接続するとともに、前記申請人装置から、前記支払い受付サーバに対して、支払い金額を指定して料金支払いを依頼するステップと、前記支払い受付サーバにより、前記申請人装置からの料金支払い依頼に応じて、金融機関に対する支払い信用照会を実施するステップと、該信用照会で前記申請人の料金支払いが保証されることが判明したときには、該料金支払いが保証される旨を示す支払い証明書を改ざん不可能な形式で作成し、前記申請人装置に送信するステップと、前記申請人装置により、送付すべき書類に前記支払い証明書を付して改ざん不可能な形式である支払い証明書付き書類とし、前記書類受付サーバに送信するステップと、前記書類受付サーバにより、前記申請人装置から送られてきた支払い証明書が未使用のものであることを確認した後、該支払い証明書付き書類を保管するステップとを備えたことを特徴とする。

【００１６】請求項６に係る発明は、ネットワーク経由で、所定の装置から書類受付サーバに対して書類を送付

する書類送付方法において、前記書類を送付する装置で、送付したい書類データに一方向関数を施して圧縮データを取得し、該圧縮データを改ざん不可能な形式で前記書類受付サーバに送信するステップと、前記書類受付サーバで、受信した圧縮データを記憶したのち、前記書類を送付する装置にチケットを送信するステップと、前記書類を送付する装置で、チケットを受信したら、送付したい書類データの前記書類受付サーバへの送信を実行するステップと、前記書類受付サーバで、前記書類データをすべて受信したら、該書類データに前記一方向関数を施して得た圧縮データと、前記記憶してある圧縮データとを比較し、それらの圧縮データが一致することを確認するステップとを備えたことを特徴とする。

【００１７】

【発明の実施の形態】以下、図面を用いて、本発明の実施の形態を説明する。

【００１８】図１は、本発明の一つの実施の形態の書類送付システムの全体図である。インターネット１１０に、書類受付サーバ１０１、支払い受付サーバ１０２、認証局１０３、代理人装置１０４、申請人装置１０５、金融機関サーバ１０６、および金融機関認証局１０７が接続されている。

【００１９】図１のシステムにおける処理の流れの概要を説明する。特に、暗号化／復号化処理やディジタル署名処理の説明は除き（それらについては後にフローチャートを参照して説明する）、データの流れに着目した処理の流れを説明する。

【００２０】申請人装置１０５は、所定の料金を支払って書類を提出したい申請人が操作する装置であり、代理人装置１０４は、その申請人を代理して書類提出（実際の書類送信）を行なう代理人が操作する装置である。提出する書類は、まず代理人が、申請人の依頼に応じて代理人装置１０４で作成する。作成した書類データは、申請人装置１０５に送信する。申請人は、受信した書類データの内容を確認し、該書類データを保存しておく。また、申請人は、申請人装置１０５から支払い受付サーバ１０２に接続し、料金支払い処理を行なう。

【００２１】支払い受付サーバ１０２は、書類提出に伴う料金の支払いに関する処理を行なうサーバであり、申請人装置１０５からの料金支払い処理要求を受けたときには、金融機関サーバ１０６に接続して当該申請人の信用照会を実施した後、支払い証明書を申請人装置１０５に返送する。支払い証明書は、申請人が料金支払いを行なったこと（あるいは、行なうことが保証されたこと）を証明するデータであり、印紙や証紙に相当するデータであるが、詳しくは後述する。支払い証明書は、書類受付サーバ１０１および支払い受付サーバ１０２の両者で共通にアクセス可能な支払い証明書管理データベース（ＤＢ）で管理される。申請人は、申請人装置１０５によりその支払い証明書を受信し、保存してあった書類データに支払い証明書を付けて代理人装置１０４に送信する。代理人は、代理人装置１０４により、該データを受信し、いったん保管する。その後任意の時期に、代理人は、該データを書類受付サーバ１０１に送信する。

【００２２】書類受付サーバ１０１は、代理人装置１０４から送信されてくる提出書類を受付るサーバである。書類受付サーバ１０１は、代理人から送信されたデータ（書類データに支払い証明書を付けたデータ）を受信し、支払い証明書を検証し書類データを保管する。支払い証明書の検証とは、当該支払い証明書が未使用のものであることを支払い証明書管理ＤＢに問い合わせ、未使用であったら使用済みにする処理である。

【００２３】認証局１０３は、申請人や代理人の認証を行なうために使用する証明書を発行する認証局である。金融機関サーバ１０６は、申請人の口座が設けられている金融機関のサーバである。金融機関認証局１０７は、その口座を持つ申請人の認証を行なうために使用する証明書を発行する認証局である。

【００２４】図２は、図１の書類受付サーバ１０１および支払い受付サーバ１０２の内部構成を示す。

【００２５】書類受付サーバ１０１は、チケット発行処理部２１１、書類受付処理部２１２、署名生成部２１３、暗号化／復号化処理部２１４、および通信制御部２１５を備えている。支払いサーバ１０２は、支払い受付処理部２２１、署名生成部２２２、暗号化／復号化処理部、支払い証明書生成管理部２２４、ＳＥＴ処理部２２５、および通信制御部２２６を備えている。また、書類受付サーバ１０１および支払いサーバ１０２の両方からアクセスできる共通データベース（ＤＢ）として、受付管理ＤＢ２３１、鍵・証明書管理ＤＢ２３２、申請人・代理人管理ＤＢ２３３、および支払い証明書管理ＤＢ２３４を備えている。

【００２６】書類受付サーバ１０１は、インターネット１１０を介して代理人装置１０４から送信されてくる書類を受付ける。書類受付処理部２１２は、その書類受付処理（図１８で詳しく説明する）を行なう。チケット発行処理部２１１は、書類受付処理を行なうにあたって、実際の書類データを受取る前にチケットを発行する処理（図１７で詳しく説明する）を行なう。チケットの発行は、書類提出日時を決定するための処理である。すなわち、代理人装置１０４から書類受付サーバ１０１に書類を送付する際に、実際に送付しようとするデータをそのまま送信すると、再送が発生してその書類提出時点があいまいになる恐れがあるので、以下の①～④のように処理して悪用を防ぐものである。

【００２７】①まず代理人装置１０４で、実際に送付しようとするデータを一方向関数で圧縮しメッセージダイジェストを求め、該メッセージダイジェストを書類受付サーバ１０１に送る。（なお、詳しくは証明書付で暗号通信を行なう。）

②書類受付サーバ１０１では、チケット発行処理部２１１によるチケット発行処理（図１７）で、新たな受付番号を取得し、該受付番号と該メッセージダイジェストを対応させて記憶するとともに、その受付番号を代理人装置１０４に送る。その受付番号を送るためのデータがチケットである。

③代理人装置１０４は、チケットにより受付番号を受取り、該受付番号を付けて実際に送付しようとするデータを、書類受付サーバ１０１に送る。

④書類受付サーバ１０１では、代理人装置１０４からのデータをすべて受信した後、そのデータを一方向関数（①で使用したのと同じ関数）で圧縮しメッセージダイジェストを求め、それが上記②で記憶してあるメッセージダイジェストと一致するか否かを確認する。一致すれば、チケット発行時に代理人装置１０４から実際に送付しようと意図していたデータが実際に受信されたことになる。一方、一致しなければ、別のデータが送信されてきたことになる。

【００２８】図８に、本実施の形態のシステムで書類受付サーバ１０１から代理人装置１０４に送られるチケットの内容を示す。受付番号８０１は、代理人装置１０４から書類送付する際に、その書類送付に対応して書類受付サーバ１０１が新たに割当てる番号である。送信者情報８０２は、その書類を送付する送信者（代理人）を特定する種々の情報である。有効期限８０３は、このチケットの有効期限を示す。代理人装置１０４から書類送付する際に、再送が発生しても当該書類の送付に十分な時間だけ有効期限（チケット発行時から所定時間を取れば良い）を取っておけばよい。無制限に遅れて書類送付されることを防ぐため、有効期限８０３を決めてある。署名８０４は、８０１～８０３のデータに対して書類受付サーバ１０１の署名を付したものである。

【００２９】図９は、本実施の形態のシステムで使用する図１の受付管理ＤＢ２３１の内容を示す。書類受付サーバ１０１は、上記②のチケット発行処理（図１７）で新たな受付番号を取得する際に、この受付管理ＤＢ２３１上で新たな受付番号を取得し、その受付番号に対応する１行分の領域を確保する。受付番号９０１、送信者情報９０２、および有効期限９０３には、送信したチケット（図８）に設定した情報８０１～８０３と同内容を記憶しておく。メッセージダイジェスト９０４、および送信者証明書９０５には、上記①で代理人装置１０４から送られてくる情報を記憶しておく。また、チケット管理情報９０６は、当該チケットが使用されたか否かのフラグ情報を記憶するもので、初期値は「未使用」にしておく。書類の内容９０７は、代理人装置１０４から送られてくる書類の全体を記憶しておく領域である。上記④でメッセージダイジェストの一致確認がなされたら、チケット管理情報９０６を「使用済み」とし、受信した書類データを書類の内容９０７に記憶するものである。

【００３０】再び、図２に戻って、書類受付サーバ１０１の構成の説明を続ける。署名生成部２１３および暗号化／復号化処理部２１４は、書類受付処理を行なうにあたって、送受するデータに署名を付すとき、および暗号化／復号化処理を行なうときに使用する。通信制御部２１５は、インターネット１１０との間の通信制御を行なう。

【００３１】支払い受付サーバ１０２は、申請人からの料金支払いを受付ける。この実施の形態のシステムでは、申請人は申請人装置１０５から支払い受付サーバ１０２に接続して、料金支払い処理を行なうことができる。支払い受付処理部２２１は、その申請人からの料金支払い要求を受付ける処理（図１３で詳しく説明する）を行ない、申請人が料金支払いを行なったこと（あるいは支払うことが保証されたこと）を示す支払い証明書を申請人に発行する。支払い証明書は、印紙や証紙、あるいは金券や商品券のような役割を果たすものである。支払い証明書の発行は、当該申請人について金融機関に対して支払い信用照会を行なった上で発行するようになっているので、書類受付け付けサーバ１０１および支払い受付サーバ１０２の運営機関は、支払い証明書を発行した金額については必ず当該申請人の口座から引き落としができる。また、支払い証明書は、予約とは異なり、あらかじめ予納口座を開く必要はない。支払い証明書は、印紙のように、別件に使用したり他人に贈与してもよい。

【００３２】図６に、本実施の形態のシステムで用いる支払い証明書の内容を示す。支払い証明書は、管理番号６０１、支払い金額６０２、申請人情報６０３、有効期限６０４、および支払い受付サーバ１０２の署名８０５を備えている。管理番号６０１は、支払い証明書に固有の管理番号である。支払い金額６０２は、申請人が支払うことを指定した金額の情報である。申請人情報８０３は、支払い要求を出して当該支払い証明書を受け取った申請人を特定する情報である。有効期限６０４は、当該支払い証明書の有効期限である。署名６０５は、当該支払い証明書を発行した支払い受付サーバ１０２の署名であり、これにより当該支払い証明書が確かに支払い受付サーバ１０２から発行されたことが保証される。これらの情報６０１～６０５は、支払い受付サーバ１０２が当該支払い証明書を発行する際に設定するものである。

【００３３】図７は、本実施の形態のシステムで使用する図１の支払い証明書管理ＤＢ２３４の内容を示す。支払い受付サーバ１０２は、発行した支払い証明書を、この支払い証明書管理ＤＢ２３４で管理する。支払い証明書管理ＤＢ２３４の７０１～７０５には、発行した支払い証明書の６０１～６０５の情報を記憶しておく。しよう状態７０６は、当該支払い証明書が使用されているか否かを示すフラグである。書類受付サーバ１０１が書類を受付けたとき、その書類に付いてきた支払い証明書の管理番号６０１で支払い証明書管理ＤＢ２３４を検索

し、対応するエントリを探す。そのエントリの使用状態７０６が「未使用」であれば、その支払い証明書は未だ使用されていなかったものであるから、その使用状態７０６を「使用済み」とする。これは印紙や証紙などの貼付を確認することに相当するものである。再度同じ支払い証明書を使った書類が送付されてきたときは、使用状態７０６が「使用済み」であるので、料金支払いが保証されていないことが確認される。

【００３４】図７のような支払い証明書管理ＤＢ２３４で支払い証明書を管理しているので、料金を支払う申請人と書類の送付を実際に実行する代理人とが異なる場合でも手続できる。また、支払い証明書を他人に譲渡して、その他人が使用することもできる。

【００３５】再び、図１に戻って、支払い受付サーバ１０２の構成の説明を続ける。署名生成部２２２および暗号化／復号化処理部は、支払い受付処理を行なうにあたって、送受するデータに署名を付すとき、および暗号化／復号化処理を行なうときに使用する。支払い証明書生成管理部２２４は、図６の構成の支払い証明書を生成し、図７の支払い証明書管理ＤＢ２３４で管理する処理を行なう。ＳＥＴ処理部２２５は、支払い受付サーバ１０２から金融機関サーバ１０６に対して申請人の信用照会を行なう際にＳＥＴプロトコルにしたがう処理を行なう。通信制御部２２６は、インターネット１１０との間の通信制御を行なう。

【００３６】書類受付サーバ１０１および支払いサーバ１０２の両方からアクセスできる共通ＤＢである受付管理ＤＢ２３１および支払い証明書管理ＤＢ２３４については、図９および図７により説明した。鍵・証明書管理ＤＢ２３２は、この書類受付サーバ１０１および支払いサーバ１０２の秘密鍵、公開鍵、および認証局１０３，１０７から発行してもらった証明書、認証を行なう際に使用する認証局１０３，１０７の公開鍵、並びに、通信相手の公開鍵などを管理するＤＢである。申請人・代理人管理ＤＢ２３３は、この書類受付サーバ１０１および支払いサーバ１０２に接続してくる申請人や代理人に関する情報を管理するＤＢである。

【００３７】なお、この実施の形態では、書類受付サーバ１０１と支払いサーバ１０２とを別装置で分け、共通ＤＢ２０３を共通に使用するような構成としたが、共通ＤＢとせず、完全にＤＢを分けて構成してもよい。その場合は、受付管理ＤＢ２３１は書類受付サーバ１０１で管理し、支払い証明書管理ＤＢ２３４は支払い受付サーバ１０２で管理すればよい。逆に、書類受付サーバ１０１および支払いサーバ１０２をＤＢ２０３も含めて１台の装置上に構成してもよい。その場合は、通信制御部、署名生成部、暗号化／復号化処理部などは共通の構成としてもよい。

【００３８】図３は、図１の認証局１０３の構成を示す。認証局１０３は、証明書発行処理部３０１、証明書管理部３０２、通信制御部３０４、および証明書管理ＤＢ３１１を備えている。認証局１０３は、あらかじめ代理人や申請人に証明書を発行する。

【００３９】図４は、図１の代理人装置１０４の構成を示す。代理人装置１０４は、申請書エディタ４０１、署名生成部４０２、暗号化／復号化処理部４０３、書類送付処理部４０４、書類受取り処理部４０５、通信制御部４０６、申請書管理ＤＢ４１１、および鍵・証明書管理ＤＢ４１２を備えている。

【００４０】申請書エディタ４０１は、送付する書類を作成するために使用するエディタである。書類送付処理部４０４は、申請人装置１０５に書類を送付する処理（図１０で詳しく説明する）や、書類受付サーバ１０１に支払い証明書付き書類を送付する処理（図１６で詳しく説明する）を行なう。書類受取り処理部４０５は、申請人から送られてくる支払い証明書付き書類の受取り処理（図１５で詳しく説明する）を行なう。署名生成部４０２および暗号化／復号化処理部４０３は、送受するデータに署名を付すとき、および暗号化／復号化処理を行なうときに使用する。通信制御部４０６は、インターネット１１０との間の通信制御を行なう。

【００４１】申請書管理ＤＢ４１１は、申請書エディタ４０１で作成した書類や、申請人から送られてくる支払い証明書付き書類を保存して管理するＤＢである。鍵・証明書管理ＤＢ４１２は、この代理人装置１０４の秘密鍵、公開鍵、および認証局１０３，１０７から発行してもらった証明書、認証を行なう際に使用する認証局１０３，１０７の公開鍵、並びに、通信相手の公開鍵などを管理するＤＢである。

【００４２】図５は、図１の申請人装置１０５の構成を示す。申請人装置１０５は、書類受取り処理部５０１、受取り書類管理部５０２、暗号化／復号化処理部５０３、署名生成部５０４、支払い処理部５０５、書類送付処理部５０６、支払い証明書管理部５０７、通信制御部５０８、申請書管理ＤＢ５１１、鍵・証明書管理ＤＢ５１２、および支払い証明書管理ＤＢ５１３を備えている。

【００４３】書類受取り処理部５０１は、代理人から送られてくる書類の受取り処理（図１１で詳しく説明する）を行なう。支払い処理部５０５は、支払い受付サーバ１０２に接続して支払いを行なう処理（図１２で詳しく説明する）を行なう。書類送付処理部５０６は、代理人に対して支払い証明書付き書類などを送付する処理（図１４で詳しく説明する）を行なう。署名生成部５０４および暗号化／復号化処理部５０３は、送受するデータに署名を付すとき、および暗号化／復号化処理を行なうときに使用する。支払い証明書管理部５０７は、支払い受付サーバ１０２から発行してもらった支払い証明書を支払い証明書管理ＤＢ５１３で管理する処理を行なう。通信制御部５０８は、インターネット１１０との間

の通信制御を行なう。

【００４４】申請書管理ＤＢ５１１は、代理人から送られてくる書類などを保存して管理するＤＢである。鍵・証明書管理ＤＢ５１２は、この申請人装置１０５の秘密鍵、公開鍵、および認証局１０３，１０７から発行してもらった証明書、認証を行なう際に使用する認証局１０３，１０７の公開鍵、並びに、通信相手の公開鍵などを管理するＤＢである。支払い証明書管理ＤＢ５１３は、支払い受付サーバ１０２から発行してもらった支払い証明書を保存して管理するＤＢである。その構成は、図７で説明した支払い受付サーバ１０２の支払い証明書管理ＤＢ２３４と同じである。ただし、支払い証明書管理ＤＢ５１３は、この申請人が受け取った支払い証明書を管理するものであり、使用状態７０６はこの申請人が使用したか否かを示す情報である。

【００４５】次に、図１０～図１８のフローチャートを参照して、図１のシステムにおける各処理の詳細を説明する。

【００４６】図１０は、代理人装置１０４から申請人装置１０５への書類送付の流れを示すフローチャートである。この処理は、主として図４の書類送付処理部４０４による処理である。まず代理人は、申請人の依頼に基づいて、図４の申請書エディタ４０１を用いて書類を作成しておく。ステップ１００１で、送付する該書類に対して代理人の電子署名を実施する。具体的には、書類データを一方向関数（ハッシュ関数など）で圧縮し、その圧縮データ（メッセージダイジェスト）を代理人の秘密鍵で暗号化した署名データを、元の書類データに付して、代理人署名付き書類を作る。次に、ステップ１００２で、代理人署名付き書類を暗号化する共通鍵を生成し、その共通鍵で代理人署名付き書類を暗号化する。次に、ステップ１００３で、申請人の公開鍵によって前記共通鍵を暗号化する。ステップ１００４では、暗号化された代理人署名付き書類と共通鍵を、代理人の証明書と共に申請人装置１０５に送信し、処理を終了する。

【００４７】なお、代理人の証明書は、あらかじめ認証局１０３から取得しておく。代理人の証明書とは、代理人の公開鍵を該代理人に関する種々の情報と連結し、該連結データに対し認証局１０３の秘密鍵で署名を付したデータである。認証局１０３は、代理人から証明書発行依頼を受けたとき、当該代理人の身元確認を行なった後、証明書を発行する。代理人装置１０４から送信するデータにこの証明書を付ければ、当該データが確かに当該代理人から送られたものであることを、この証明書によって検証することができ、またこの証明書から代理人の公開鍵や代理人を特定する種々の情報を取得することができる。同様にして、申請人も、あらかじめ認証局１０３から証明書を取得しておく。

【００４８】図１１は、図１０の処理により代理人装置１０４から申請人装置１０５へ送られたデータを受取る申請人装置１０５の処理の流れを示す。この処理は、主として図５の書類受取り処理部５０１による処理である。まずステップ１１０１で、受信データ中の代理人の証明書を検証するとともに、受信データ中の暗号化された共通鍵を申請人の秘密鍵を用いて復号化する。ステップ１１０２で、復号化された共通鍵を用いて、代理人署名付き書類を復号化する。ステップ１１０３では、その代理人署名付き書類の署名を代理人の公開鍵を用いて検証する。この検証は、署名データを代理人の公開鍵で復号化した値が、書類データを一方向関数（図１０のステップ１００１で使用したのと同じ関数を用いる）で圧縮した圧縮データ（メッセージダイジェスト）に等しくなるか否かを確認する処理である。検証の結果、適正な署名であったら、ステップ１１０５で当該代理人署名付き書類を保管する。検証の結果、適正な署名でなかったら、ステップ１１０６で申請書類が改ざんされていることを申請人に報告して、処理を終了する。

【００４９】図１２は、申請人による料金支払い処理の流れを示すフローチャートである。この処理は、主として図５の支払い処理部５０５による処理である。まずステップ１２０１で、申請人装置１０５から支払い受付サーバ１０２に接続し、支払い金額を決定・送信する。ステップ１２０２で、申請人の証明書（認証局１０３から取得した証明書）を支払い受付サーバ１０２に提示する。ステップ１２０３は、支払い受付サーバ１０２側の処理であり、図１３で後述するが、支払い受付サーバ１０２からは、申請人の公開鍵で暗号化された共通鍵と該共通鍵で暗号化された支払い証明書（図６）が送信されてくる。ステップ１２０４では、支払い受付サーバ１０２から送信された暗号化された共通鍵を申請人の秘密鍵で復号化する。ステップ１２０５では、復号化された共通鍵を用いて、暗号化された支払い証明書を復号化する。ステップ１２０６で、復号化された支払い証明書を、支払い証明書管理ＤＢ５１３（図７）に保管して、処理を終了する。

【００５０】図１３は、図１２のステップ１２０３の処理、すなわち支払い受付サーバ１０２における支払い受付処理の流れを示すフローチャートである。この処理は、主として図２の支払い受付処理部２２１による処理である。まず、ステップ１３０１で、申請人から送られた証明書を検証し、申請人の公開鍵を取得する。次にステップ１３０２で、例えばＳＥＴのプロトコルを用いて、申請人からの支払い信用照会（与信）を金融機関に対して実施する。具体的には、図１の金融機関サーバ１０６に申請人と引き落とし金額を特定する情報を送信し、該申請人の口座からその引き落とし金額分を確保する。

【００５１】なお、金融機関に対して支払い信用照会を実施する際、支払い受付サーバ１０２を運営する機関の身元を証明するため、あらかじめ支払い受付サーバ１０

２を運営する機関は、金融機関認証局１０７から証明書を取得しておく必要がある。また、この支払い信用照会では、引き落とし を行なう申請人についての認証も行なうので（確かにその申請人からの引き落とし依頼であるかどうかを確認する必要がある）、あらかじめ申請人は金融機関認証局１０７から証明書を取得しておくとともに、その金融機関の証明書をステップ１２０２で支払い受付サーバ１０２に送り、支払い受付サーバ１０２はステップ１３０２で信用照会するときその申請人の金融機関の証明書を付けて信用照会する必要がある。

【００５２】ステップ１３０２の信用照会の結果、ステップ１３０３で、上記引き落とし金額分の引き落とし枠が確保できたらステップ１３０４に進む。信用照会結果に何らかの問題があったら、処理を終了する。ステップ１３０４では、新たに発行する支払い証明書の管理番号を取得する。具体的には、図７の構成の支払い証明書管理ＤＢ２３４で新規管理番号の一行分の領域を確保する。次に、ステップ１３０５で、申請人の証明書から申請人を特定する情報を抽出する。ステップ１３０６では、管理番号、支払い金額、申請人を特定する情報、および有効期限を連結したデータに電子署名を実施して、支払い証明書（図６）を作成する。具体的には、上記連結データを一方向関数（ハッシュ関数など）で圧縮し、その圧縮データを支払い受付サーバ１０２の秘密鍵で暗号化した署名データを、元の連結データに付して、支払い証明書を作る。

【００５３】ステップ１３０７では、作成した支払い証明書に含めた情報を支払い証明書管理ＤＢ２３４（図７）に記録する。そして、ステップ１３０８で、支払い証明書を暗号化するための共通鍵を生成し、その共通鍵で支払い証明書を暗号化する。次に、ステップ１３０９で、申請人の公開鍵によって前記共通鍵を暗号化する。ステップ１３１０では、暗号化された共通鍵と該共通鍵で暗号化された支払い証明書とを申請人装置１０５に送信し、処理を終了する。

【００５４】図１４は、申請人装置１０５から代理人装置１０４への書類送付の流れを示すフローチャートである。この処理は、主として図５の書類送付処理部５０６による処理である。まずステップ１４０１で、図１１のステップ１１０５で保管してある代理人署名付き書類を取り出す。ステップ１４０２では、代理人署名付き書類と支払い証明書とを含めたデータに対して、申請人の電子署名を実施する。これを支払い証明書付き書類と呼ぶ。なお、ここで使用する支払い証明書は、図７の構成の支払い証明書管理ＤＢ５１３で管理されている支払い証明書のうち、使用状況７０６が「未使用」のものを使用する。使用した支払明細書の使用状況７０６は「使用済み」に変更しておく。

【００５５】次に、ステップ１４０３で、共通鍵を生成し、該共通鍵で支払い証明書付き書類を暗号化する。ステップ１４０４で、代理人の公開鍵を用いて、前記共通鍵を暗号化する。ステップ１４０５では、暗号化された共通鍵と該共通鍵で暗号化された支払い証明書付き書類を代理人装置１０４に送信する。

【００５６】図１５は、図１４で送信された申請人からのデータを受取る代理人装置１０４の処理の流れを示すフローチャートである。この処理は、主として図４の書類受取り処理部４０５による処理である。まずステップ１５０１で、受信データ中の暗号化された共通鍵を代理人の秘密鍵を用いて復号化する。ステップ１５０２で、復号化された共通鍵を用いて、支払い証明書付き書類を復号化する。ステップ１５０３では、その支払い証明書付き書類に添付されている申請人の電子署名を申請人の公開鍵を用いて検証する。この検証は、署名データを申請人の公開鍵で復号化した値が、支払い証明書付き書類を一方向関数（図１４のステップ１４０２の署名で使用したのと同じ関数）で圧縮した圧縮データに等しくなるか否かを確認する処理である。

【００５７】ステップ１５０４で、検証の結果、適正な署名であったら、ステップ１５０６に進む。ステップ１５０６では、支払い証明書付き書類に含まれている支払い証明書の電子署名を支払い受付サーバ１０２の公開鍵を用いて検証する。この検証は、署名データを支払い受付サーバ１０２の公開鍵で復号化した値が、支払い証明書に含まれている管理番号、支払い金額、申請人を特定する情報、および有効期限を連結したデータを一方向関数（図１３のステップ１３０６の署名で使用したのと同じ関数）で圧縮した圧縮データに等しくなるか否かを確認する処理である。

【００５８】ステップ１５０７で、検証の結果、適正な署名であったら、ステップ１５０９に進む。ステップ１５０９では、支払い証明書付き書類に含まれている代理人署名付き書類中の代理人の署名を、代理人の秘密鍵を用いて検証する。ステップ１５１０で検証結果が適正な署名であったら、ステップ１５１２で支払い証明書付き書類を保管して、処理を終了する。ステップ１５０４，１５０７，１５１０の何れかのステップで、検証結果が不正な署名であることを示していたら、それぞれ、ステップ１５０５，１５０８，１５１１で書類が改ざんされていることを代理人に報告して、処理を終了する。

【００５９】図１６は、代理人装置１０４から書類受付サーバ１０１への支払い証明書付き書類の送付処理の流れを示すフローチャートである。この処理は、主として図４の書類送付処理部４０４による処理である。まずステップ１６０１で、送付しようとする支払い証明書付き書類を一方向関数で圧縮し、圧縮データ（メッセージダイジェスト）を生成する。次に、ステップ１６０２で、共通鍵を生成し、該共通鍵で上記メッセージダイジェストを暗号化する。ステップ１６０３では、上記共通鍵を書類受付サーバ１０１の公開鍵で暗号化する。ステップ

１６０４では、暗号化された共通鍵と該共通化鍵で暗号化されたメッセージダイジェストに、代理人の証明書を添付して書類受付サーバ１０１に送付する。ステップ１６０５は、書類受付サーバ１０１側のチケット発行処理であり、図１７で後述するが、書類受付サーバ１０１からは、代理人の公開鍵で暗号化された共通鍵（書類受付サーバ１０１側で生成した鍵）と該共通鍵で暗号化されたチケット（図８）が送信されてくる。

【００６０】ステップ１６０６では、書類受付サーバ１０１から送られてきた暗号化された共通鍵を、代理人の秘密鍵を用いて復号化する。ステップ１６０７では、復号化された共通鍵を用いてチケットを復号化する。次に、ステップ１６０８で、書類受付サーバ１０１の公開鍵を用いて、チケット（図８）に付いている電子署名を検証する。ステップ１６０９で、検証結果が適正な署名であることを示していたら、書類受付サーバ１０１が提出日時を確保したということであるから、ステップ１６１１に進む。ステップ１６０９で、不正な署名であったら、ステップ１６１０でチケットが改ざんされていることを代理人に報告し、処理を終了する。

【００６１】チケットが取れたら、ステップ１６１１で共通鍵を生成し、ステップ１６１２で支払い証明書付き書類を該共通鍵で暗号化する。ステップ１６１３では、該共通鍵でチケットを暗号化する。次に、ステップ１６１４で、書類受付サーバ１０１の公開鍵で上記共通鍵を暗号化する。そして、ステップ１６１５で、暗号化した共通鍵、および該共通鍵で暗号化したチケットと支払い証明書付き書類を書類受付サーバ１０１に送付する。ステップ１６１６は、書類受付サーバ１０１側の処理であり、図１８で後述するが、書類受付サーバ１０１からは、代理人の公開鍵で暗号化された共通鍵と該共通鍵で暗号化された受付確認書が送信されてくる。

【００６２】ステップ１６１７では、書類受付サーバ１０１から送信された暗号化された共通鍵を代理人の秘密鍵で復号化する。ステップ１６１８では、復号化された共通鍵を用いて、暗号化された受付確認書を復号化する。ステップ１６１９で、受付確認書に添付された書類受付サーバ１０１の電子署名を検証する。ステップ１６２０で検証結果が適正な署名であることを示していたら、ステップ１６２２で、受付確認書を保管して、処理を終了する。ステップ１６２０で、検証結果が不正な署名であることを示していたら、ステップ１６２０で何らかのデータ改ざんがなされたことを代理人に報告し、処理を終了する。

【００６３】図１７は、図１６のステップ１６０５の処理、すなわち書類受付サーバ１０１のチケット発行処理の流れを示すフローチャートである。この処理は、主として図２のチケット発行処理部２１１による処理である。まずステップ１７０１で、書類受付サーバ１０１の秘密鍵を用いて、代理人から送られてきた共通鍵を復号化する。次に、ステップ１７０２で、該共通鍵を用いてメッセージダイジェストを復号化する。そして、ステップ１７０３で、新たな受付番号を取得し、該受付番号９０１、代理人（送信者）に関する情報９０２、有効期限９０３、メッセージダイジェスト９０４、および代理人の証明書９０５を、受付管理ＤＢ２３１（図９）に保管する。なお、代理人に関する情報は、代理人から送られてきたデータに含まれている代理人の証明書から抽出した情報を設定する。有効期限は、現時点に所定時間を加えた時間を設定する。また、チケットの管理情報９０６は「未使用」に初期化しておく。

【００６４】次に、ステップ１７０４では、受付番号と、代理人に関する情報と、有効期限とを連結したデータを生成し、該連結データに対して電子署名を実施する。この電子署名付きデータがチケット（図８）である。具体的には、上記連結データを一方向関数（図１６のステップ１６０１や１６０８で用いたのと同じ関数）で圧縮し、その圧縮データを書類受付サーバ１０１の秘密鍵で暗号化した署名データを、元の連結データに付して、チケット（図８）を作る。次に、ステップ１７０５で、共通鍵を生成し、該共通鍵で上記チケットを暗号化する。ステップ１７０６では、代理人の公開鍵を用いて、上記共通鍵を暗号化する。ステップ１７０７で、暗号化された共通鍵、および該共通鍵で暗号化されたチケットを代理人に対して送付し、処理を終了する。

【００６５】図１８は、図１６のステップ１６１６の処理、すなわち書類受付サーバ１０１による書類受付処理の流れを示すフローチャートである。この処理は、主として図２の書類受付処理部２１２により実行される処理である。まずステップ１８０１で、書類受付サーバ１０１の秘密鍵を用いて、代理人から送られてきた共通鍵を復号化する。ステップ１８０２で、復号化された共通鍵を用いて、チケットと支払い証明書付き書類を復号化する。次に、ステップ１８０３で、チケットに付いている電子署名、および有効期限を検証する。検証の結果、ステップ１８０４で、署名も適正で有効期限内であるときは、ステップ１８０６に進む。署名が不正、または有効期限が過ぎていた場合は、ステップ１８０５でチケット不正を表示して、処理を終了する。

【００６６】ステップ１８０６では、代理人から送付されてきた支払い証明書付き書類を、代理人装置１０４で使用した一方向関数（図１６のステップ１６０１や１６０８で用いたのと同一の関数）で圧縮し、メッセージダイジェストを生成する。ステップ１８０７では、代理人から送付されてきたチケットから受付番号を取り出し、受付管理ＤＢ２３１（図９）を参照して、当該受付番号に対応するチケット請求時のメッセージダイジェストを取り出し、ステップ１８０６で生成したメッセージダイジェストと比較する。比較の結果、ステップ１８０８で同一であれば、確かにチケット請求時に送ろうとしてい

た内容が送られてきたものと認められるので、ステップ１８１０に進む。ステップ１８０８で比較の結果が同一でないときは、チケット請求時に送ろうとしていた内容と別の内容が送られてきたということだから、ステップ１８０９で送付データ不一致の表示を行ない、処理を終了する。

【００６７】ステップ１８１０では、支払い証明書に含まれている管理番号のデータを支払い証明書管理ＤＢ２３４（図７）から検索し、その使用状況７０６が「未使用」であるか否かを検証する。ステップ１８１１で、「未使用」であったときは、ステップ１８１３で、支払い証明書管理ＤＢ２３４の当該管理番号の支払い証明書の使用状況７０６を「使用済み」に変更する。次に、ステップ１８１４で、当該受付番号のチケットの管理情報９０６を「使用済み」に変更する。そして、ステップ１８１５で、支払い証明書付き書類を保管する。書類の保管は、図９の受付管理ＤＢ２３１の書類の内容９０７に格納することにより行なう。

【００６８】さらに、ステップ１８１６で、受付番号などの受付情報を含む受付確認書を作成し、電子署名を実行する。ステップ１８１７で、共通鍵を生成し、該共通鍵で上記電子署名付き受付確認書を暗号化する。ステップ１８１８では、代理人の公開鍵で上記共通鍵を暗号化する。ステップ１８１９で、暗号化した共通鍵、および該共通鍵で暗号化した電子署名付き受付確認書を代理人に送付して、処理を終了する。

【００６９】上記実施の形態のシステムによれば、申請人が支払い証明書を取得し、代理人が提出書類に支払い証明書を付けて、書類受付サーバに送付することが可能になる。支払い証明書は、印紙や証紙、金券や商品券のようなイメージで使用することができ、支払い受付サーバの署名が付いているので容易に改ざんされない。実際の決済はどのような形態で行なってもよいが、与信の段階で引き落とし可能であることが保証されるので、書類受付サーバの側では必ず料金を徴収できる。また、申請人が書類と支払い証明書を付けて、その全体に署名を付して、代理人に送っているので、申請人が当該書類の内容で了解しているという意志表示をしたことになるし、その後代理人が書類を改ざんすることもできない。

【００７０】さらに、書類提出時点を決定する際、始めに提出者から送付しようとする書類データを一方向関数で圧縮してメッセージダイジェストを求め、これを証明書と一緒に書類受付サーバに送り、書類受付サーバではそのメッセージダイジェストを記憶して、チケットを返す。その後、提出者から書類データの全体が送られてきたときには、そのメッセージダイジェストを求めて、チケット発行時に記憶してあるメッセージダイジェストと比較することで、当初から送る予定の書類が確かに送られてきたことを確認できる。そのため、チケット発行時を書類提出時点とみなすことができるようになる。

【００７１】なお、上記実施の形態では、代理人が申請者を代理して書類提出を行なう例を説明したが、代理人経由でなく、直接、申請人が書類受付サーバに対する書類送付を行なうようにしてもよい。

【００７２】また、上記実施の形態では、支払方式としてＳＥＴを用いた例を説明したが、ＳＥＴ以外の支払方式、例えばＳＥＴを使わないクレジットカード支払いの方式などを用いてもよい。

【００７３】本発明は、特許庁、登記所、あるいは役所などの官公庁に対してインターネット経由で書類を送付する場合などに適用可能である。また、いわゆる電子ショッピングなどに適用することも可能である。

【００７４】

【発明の効果】以上説明したように、本発明によれば、インターネットなどを介して通信で電子的な書類提出を行なう際に手数料の支払いが必要な場合において、支払い受付サーバに対して支払い依頼を出せば、支払い受付サーバが信用照会を実施し、料金の支払いが保証される場合にはその旨を示す改ざん不可能な形式の支払い証明書を発行してくれるので、于銭口座のような特別な口座を作る必要が無く、クレジットカードや銀行口座から別フェーズで引き落とし処理を行なう場合に引き落とせないというようなことも無く、また料金を支払う者と書類の提出を行なう者とが異なる場合でも適正に書類提出とその料金支払いを行なうことができる。

【００７５】また、書類を送付する前に、送付する書類を一方向関数で圧縮した圧縮データを送り、あとで実際に送られてきた書類に対して同じ一方向関数で圧縮した圧縮データと比較確認しているので、通信で電子的な書類提出を行なう場合に、悪用を許すことなく、提出日時を合理的に決定する仕組みが提供される。

【図面の簡単な説明】

【図１】本発明の実施の形態の書類送付システムの全体図

【図２】書類受付サーバおよび支払い受付サーバの内部構成図

【図３】認証局の構成図

【図４】代理人装置の構成図

【図５】申請人装置の構成図

【図６】本実施の形態のシステムで用いる支払い証明書の内容を示す図

【図７】本実施の形態のシステムで使用する支払い証明書管理ＤＢの内容を示す図

【図８】本実施の形態のシステムで書類受付サーバから代理人装置に送られるチケットの内容を示す図

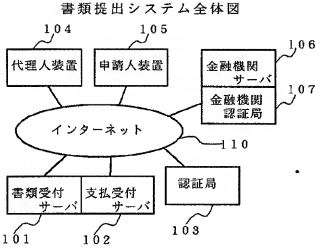
【図９】本実施の形態のシステムで使用する受付管理ＤＢの内容を示す図

【図１０】代理人装置から申請人装置への書類送付の流れを示すフローチャート図

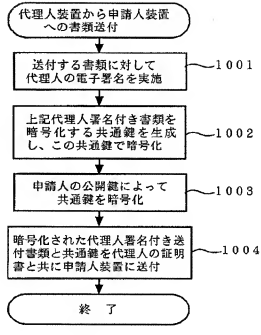
【図１１】代理人装置から申請人装置へ送られたデータ

を受取る申請人装置の処理の流れを示すフローチャート図
【図１２】申請人による料金支払い処理の流れを示すフローチャート図
【図１３】支払い受付サーバにおける支払い受付処理の流れを示すフローチャート図
【図１４】申請人装置から代理人装置への書類送付の流れを示すフローチャート図
【図１５】申請人からのデータを受取る代理人装置の処理の流れを示すフローチャート図
【図１６】代理人装置から書類受付サーバへの支払い証＊明書付き書類の送付処理の流れを示すフローチャート図
【図１７】書類受付サーバのチケット発行処理の流れを示すフローチャート図
【図１８】書類受付サーバによる書類受付処理の流れを示すフローチャート図
【符号の説明】
１０１…書類受付サーバ、１０２…支払い受付サーバ、１０３…認証局、１０４…代理人装置、１０５…申請人装置、１０６…金融機関サーバ、１０７…金融機関認証局、１１０…インターネット。

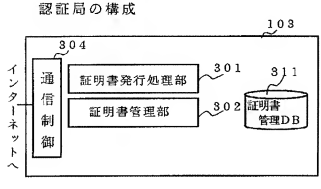
【図１】



【図１０】

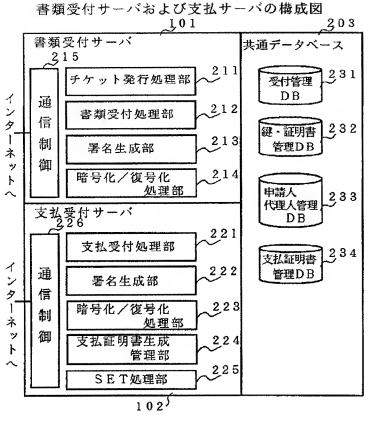


【図３】



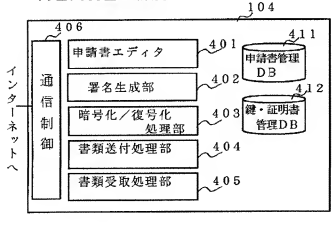
【図２】

書類受付サーバおよび支払サーバの構成図

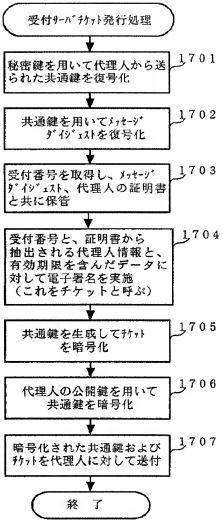


【図４】

代理人装置の構成

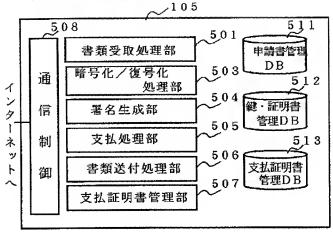


【図１７】



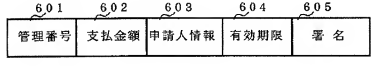
【図５】

申請人装置の構成



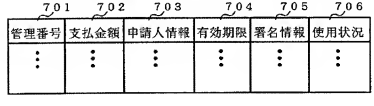
【図６】

支払証明書の内容



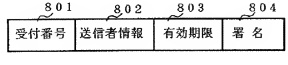
【図７】

支払証明書管理ＤＢの内容



【図８】

チケットの内容

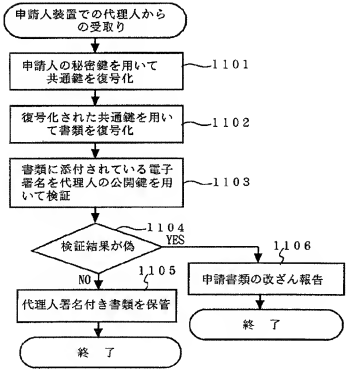


【図９】

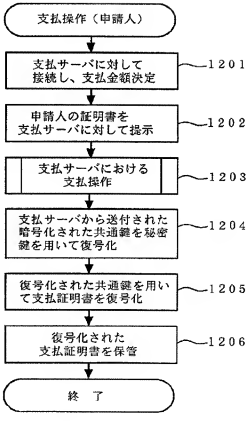
受付管理ＤＢの内容

901 受付番号	902 送信者情報	903 有効期限	904 メッセージダイジェスト	905 送信者証明書	906 チケット管理情報	907 書類の内容
⋮	⋮	⋮	⋮	⋮	⋮	⋮

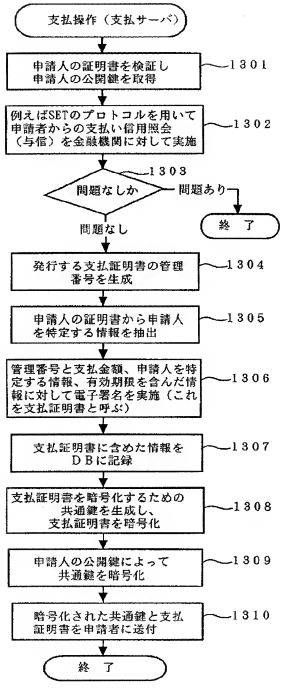
【図１１】



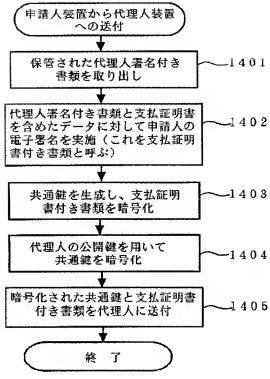
【図１２】



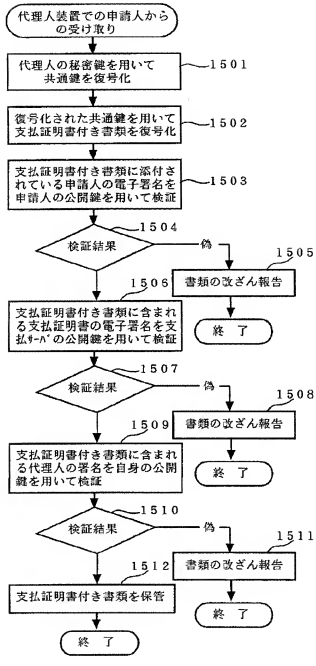
【図１３】


支払操作（支払サーバ）
申請人の証明書を検証し
申請人の公開鍵を取得
1301
例えばSETのプロトコルを用いて
申請者からの支払い信用照会
（与信）を金融機関に対して実施
1302
1303
問題なしか
問題あり
終　了
問題なし
発行する支払証明書の管理
番号を生成
1304
申請人の証明書から申請人
を特定する情報を抽出
1305
管理番号と支払金額、申請人を特
定する情報、有効期限を含んだ情
報に対して電子署名を実施（これ
を支払証明書と呼ぶ）
1306
支払証明書に含めた情報を
ＤＢに記録
1307
支払証明書を暗号化するための
共通鍵を生成し、
支払証明書を暗号化
1308
申請人の公開鍵によって
共通鍵を暗号化
1309
暗号化された共通鍵と支払
証明書を申請者に送付
1310
終　了

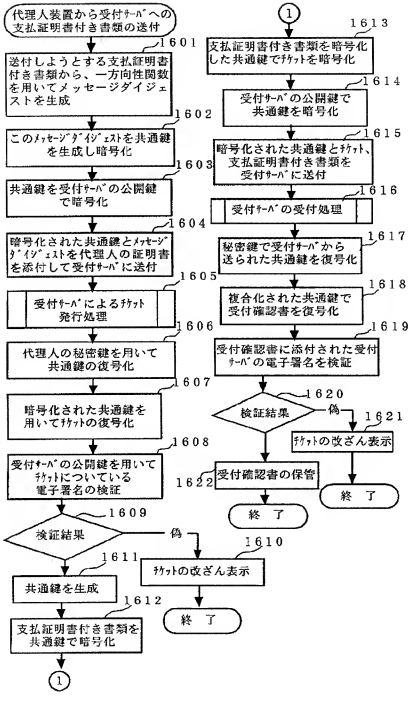
【図１４】


申請人装置から代理人装置への送付
保管された代理人署名付き書類を取り出し
１４０１
代理人署名付き書類と支払証明書を含めたデータに対して申請人の電子署名を実施（これを支払証明書付き書類と呼ぶ）
１４０２
共通鍵を生成し、支払証明書付き書類を暗号化
１４０３
代理人の公開鍵を用いて共通鍵を暗号化
１４０４
暗号化された共通鍵と支払証明書付き書類を代理人に送付
１４０５
終　了

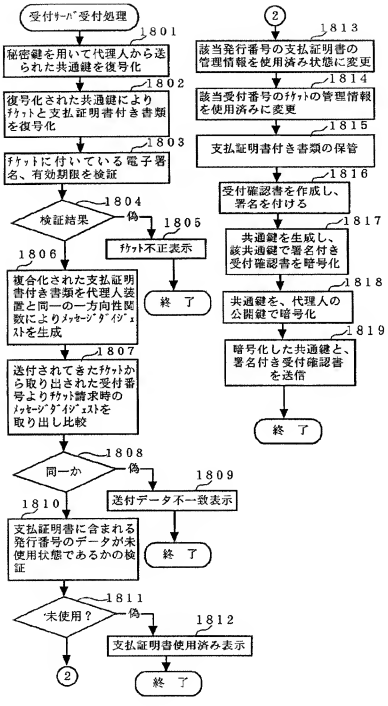
【図１５】


代理人装置での申請人からの受け取り
代理人の秘密鍵を用いて共通鍵を復号化
1501
復号化された共通鍵を用いて支払証明書付き書類を復号化
1502
支払証明書付き書類に添付されている申請人の電子署名を申請人の公開鍵を用いて検証
1503
1504
検証結果
偽
1505
書類の改ざん報告
終　了
1506
支払証明書付き書類に含まれる支払証明書の電子署名を支払ｾﾝﾀｰの公開鍵を用いて検証
1507
検証結果
偽
1508
書類の改ざん報告
終　了
1509
支払証明書付き書類に含まれる代理人の署名を自身の公開鍵を用いて検証
1510
検証結果
偽
1511
書類の改ざん報告
終　了
1512
支払証明書付き書類を保管
終　了

【図１６】


代理人装置から受付ｻｰﾊﾞへの支払証明書付き書類の送付
1601
送付しようとする支払証明書付き書類から、一方向性関数を用いてメッセージダイジェストを生成
1602
このﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄを共通鍵を生成し暗号化
1603
共通鍵を受付ｻｰﾊﾞの公開鍵で暗号化
1604
暗号化された共通鍵とﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄを代理人の証明書を添付して受付ｻｰﾊﾞに送付
1605
受付ｻｰﾊﾞによるﾁｹｯﾄ発行処理
1606
代理人の秘密鍵を用いて共通鍵の復号化
1607
暗号化された共通鍵を用いてﾁｹｯﾄの復号化
1608
受付ｻｰﾊﾞの公開鍵を用いてﾁｹｯﾄについている電子署名の検証
1609
検証結果
偽
1610
ﾁｹｯﾄの改ざん表示
終了
1611
共通鍵を生成
1612
支払証明書付き書類を共通鍵で暗号化
①
①
1613
支払証明書付き書類を暗号化した共通鍵でﾁｹｯﾄを暗号化
1614
受付ｻｰﾊﾞの公開鍵で共通鍵を暗号化
1615
暗号化された共通鍵とﾁｹｯﾄ、支払証明書付き書類を受付ｻｰﾊﾞに送付
1616
受付ｻｰﾊﾞの受付処理
1617
秘密鍵で受付ｻｰﾊﾞから送られた共通鍵を復号化
1618
複合化された共通鍵で受付確認書を復号化
1619
受付確認書に添付された受付ｻｰﾊﾞの電子署名を検証
1620
検証結果
偽
1621
ﾁｹｯﾄの改ざん表示
終了
1622
受付確認書の保管
終了

【図１８】


受付ｻｰﾊﾞ受付処理
1801
秘密鍵を用いて代理人から送られた共通鍵を復号化
1802
復号化された共通鍵によりﾁｹｯﾄと支払証明書付き書類を復号化
1803
ﾁｹｯﾄに付いている電子署名、有効期限を検証
1804
検証結果
偽
1805
ﾁｹｯﾄ不正表示
終　了
1806
複合化された支払証明書付き書類を代理人装置と同一の一方向性関数によりﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄを生成
1807
送付されてきたﾁｹｯﾄから取り出された受付番号よりﾁｹｯﾄ請求時のﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄを取り出し比較
1808
同一か
偽
1809
送付データ不一致表示
終　了
1810
支払証明書に含まれる発行番号のデータが未使用状態であるかの検証
1811
未使用？
偽
1812
支払証明書使用済み表示
終　了
2
2
1813
該当発行番号の支払証明書の管理情報を使用済み状態に変更
1814
該当受付番号のﾁｹｯﾄの管理情報を使用済みに変更
1815
支払証明書付き書類の保管
1816
受付確認書を作成し、署名を付ける
1817
共通鍵を生成し、該共通鍵で署名付き受付確認書を暗号化
1818
共通鍵を、代理人の公開鍵で暗号化
1819
暗号化した共通鍵と、署名付き受付確認書を送信
終　了

【公報種別】特許法第１７条の２の規定による補正の掲載
【部門区分】第６部門第３区分
【発行日】平成１３年２月２３日（２００１．２．２３）

【公開番号】特開平１１－１７５６０７
【公開日】平成１１年７月２日（１９９９．７．２）
【年通号数】公開特許公報１１－１７５７
【出願番号】特願平９－３５２２４３
【国際特許分類第７版】
　G06F　17/60
【Ｆ１】
　G06F　15/21　　Z

【手続補正書】
【提出日】平成１１年９月１０日（１９９９．９．１０）
【手続補正１】
【補正対象書類名】明細書
【補正対象項目名】発明の名称
【補正方法】変更
【補正内容】
【発明の名称】　データ送付方法、装置及びシステム並びにその方法を格納した記録媒体
【手続補正２】
【補正対象書類名】明細書
【補正対象項目名】特許請求の範囲
【補正方法】変更
【補正内容】
【特許請求の範囲】
【請求項１】ネットワークで接続された第１、第２、第３の計算機を有し、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付方法であって、前記第１の計算機から前記第３の計算機に対して認証を依頼するステップと、前記第１の計算機からの認証依頼に応じて、前記第３の計算機で認証を行い、当該認証の結果に応じて、認証済みである旨の証明書データを作成し、前記第１の計算機に送付するステップと、前記第３の計算機からの証明書データを受けて、前記第１の計算機で送付する電子化データに前記証明書データを付して証明書付きデータとし、前記第２の計算機に送付するステップと、前記第１の計算機からの証明書付きデータを受けて、前記第２の計算機で証明書データが未使用のものであることを確認し、当該証明書付きデータを保管するステップとを備えたことを特徴とするデータ送付方法。
【請求項２】第１、第２、第３の計算機が接続されたネットワークを利用し、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付方法であって、前記第１の計算機から前記第３の計算機に対して認証を依頼するステップと、前記第３の計算機から認証結果を受け、前記第２の計算機に送付する電子化データに前記認証結果を付した認証付きデータとし、前記第２の計算機に送付するステップとを備えたことを特徴とするデータ送付方法。
【請求項３】ネットワーク経由で、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付方法であって、前記第１の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第２の計算機に送付するステップと、前記電子化データを前記第２の計算機に送付するステップと、前記第２の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップとを備えたことを特徴とするデータ送付方法。
【請求項４】ネットワーク経由で、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付方法であって、前記第１の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第２の計算機に送付するステップと、前記第２の計算機で、前記圧縮データを受信後、前記第１の計算機に受信を示す受信済みデータを送付するステップと、前記第１の計算機で、前記受信済みデータを受信後、前記電子化データを前記第２の計算機に送付するステップと、前記第２の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップとを備えたことを特徴とするデータ送付方法。
【請求項５】ネットワーク経由で、他の計算機に対して電子化データを送付するデータ送付方法であって、前記電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記他の計算機に送付するステップと、前記他の計算機から前記圧縮データを受信した旨の通知を受けて、前記電子化データを前記他の計算機に送付するステップとを備えたことを特徴とするデータ送付方法。
【請求項６】ネットワークで接続された第１、第２、第３の計算機を有し、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付システムであって、前記第１の計算機は、前記第３の計算機に対して認

証を依頼する手段を備え、前記第３の計算機は、前記第１の計算機からの認証依頼に応じて認証を行う手段と、当該認証の結果に応じて、認証済みである旨の証明書データを作成し、前記第１の計算機に送付する手段とを備え、前記第１の計算機は、前記第３の計算機からの証明書データを受けて、電子化データに前記証明書データを付して証明書付きデータとし、前記第２の計算機に送付する手段を備え、前記第２の計算機は、前記第１の計算機からの証明書付きデータを受けて、証明書データが未使用のものであることを確認し、当該証明書付きデータを保管する手段を備えたことを特徴とするデータ送付システム。

【請求項７】第１、第２の計算機が接続されたネットワークを利用して、前記第１の計算機へ電子化データを送付するデータ送付装置であって、前記第２の計算機に対して認証を依頼する手段と、前記第２の計算機から認証結果を受けとる手段と、前記第１の計算機に送付する電子化データに前記認証結果を付した認証付きデータを作成する手段と、当該認証付きデータを前記第１の計算機に送付する手段とを備えたことを特徴とするデータ送付装置。

【請求項８】ネットワーク経由で、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付システムであって、前記第１の計算機は、電子化データを圧縮した圧縮データを作成する手段と、当該圧縮データを前記第２の計算機に送付する手段と、前記電子化データを前記第２の計算機に送付する手段とを備え、前記第２の計算機は、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較する手段とを備えたことを特徴とするデータ送付システム。

【請求項９】ネットワーク経由で、他の計算機に対して電子化データを送付するデータ送付装置であって、前記電子化データを圧縮した圧縮データを作成する手段と、当該圧縮データを前記他の計算機に送付する手段と、前記他の計算機から前記圧縮データを受信した旨の通知を受けて、前記電子化データの前記他の計算機への送付を実行する手段とを備えたことを特徴とするデータ送付装置。

【請求項１０】第１の計算機から第２の計算機に対して電子化データを送付するデータ送付方法を実現するプログラムを格納した記録媒体であって、前記データ送付方法は以下を含む：前記第１の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第２の計算機に送付するステップと、前記電子化データを前記第２の計算機に送付するステップと、前記第２の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップ。

【手続補正３】
【補正対象書類名】明細書
【補正対象項目名】０００１
【補正方法】変更
【補正内容】
【０００１】
【発明の属する技術分野】本発明は、電子データで各種の書類を送付・受付し、該書類の送付・受付に伴う料金の支払いやその支払い受付を行なうデータ送付方法、装置及びシステム並びにその方法を格納した記録媒体に関する。

【手続補正４】
【補正対象書類名】明細書
【補正対象項目名】０００９
【補正方法】変更
【補正内容】
【０００９】本発明は、上述の従来形における問題点に鑑み、インターネットなどを介して通信で電子的な書類提出を行なう際に手数料の支払いが必要な場合において、予納口座のような特別な口座を作る必要が無く、クレジットカードや銀行口座から別フェーズで引き落とし処理を行なうことも無く、また料金を支払う者と書類の提出を行なう者とが異なる場合でも適正に書類提出とその料金支払いを行なうことができるデータ送付方法、装置及びシステム並びにその方法を格納した記録媒体を提供することを目的とする。

【手続補正５】
【補正対象書類名】明細書
【補正対象項目名】００１０
【補正方法】変更
【補正内容】
【００１０】また、本発明は、通信で電子的な書類提出を行なう場合に、悪用を許すことなく、提出日時を合理的に決定する仕組みを備えたデータ送付方法、装置及びシステム並びにその方法を格納した記録媒体を提供することを目的とする。

【手続補正６】
【補正対象書類名】明細書
【補正対象項目名】００１１
【補正方法】変更
【補正内容】
【００１１】【課題を解決するための手段】上記目的を達成するため、本発明は、ネットワークで接続された第１、第２、第３の計算機を有し、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付方法であって、前記第１の計算機から前記第３の計算機に対して認証を依頼するステップと、前記第１の計算機からの認証依頼に応じて、前記第３の計算機で認証を行い、当該認証の結果に応じて、認証済みである旨の証明書データを作成し、前記第１の計算機に送付するステップと、前記第３の計算機からの証明書データを受けて、前記第１の計算機で送付する電子化データに前記証明書データを付

して証明書付きデータとし、前記第２の計算機に送付するステップと、前記第１の計算機からの証明書付きデータを受けて、前記第２の計算機で証明書データが未使用のものであることを確認し、当該証明書付きデータを保管するステップとを備えたことを特徴とする。

【手続補正７】
【補正対象書類名】明細書
【補正対象項目名】００１２
【補正方法】変更
【補正内容】
【００１２】また本発明は、第１、第２、第３の計算機が接続されたネットワークを利用し、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付方法であって、前記第１の計算機から前記第３の計算機に対して認証を依頼するステップと、前記第３の計算機から認証結果を受け、前記第２の計算機に送付する電子化データに前記認証結果を付した認証付きデータとし、前記第２の計算機に送付するステップとを備えたことを特徴とする。

【手続補正８】
【補正対象書類名】明細書
【補正対象項目名】００１３
【補正方法】変更
【補正内容】
【００１３】また本発明は、ネットワーク経由で、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付方法であって、前記第１の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第２の計算機に送付するステップと、前記電子化データを前記第２の計算機に送付するステップと、前記第２の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップとを備えたことを特徴とする。

【手続補正９】
【補正対象書類名】明細書
【補正対象項目名】００１４
【補正方法】変更
【補正内容】
【００１４】また本発明は、ネットワーク経由で、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付方法であって、前記第１の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第２の計算機に送付するステップと、前記第２の計算機で、前記圧縮データを受信後、前記第１の計算機に受信を示す受信済みデータを送付するステップと、前記第１の計算機で、前記受信済みデータを受信後、前記電子化データを前記第２の計算機に送付するステップと、前記第２の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップとを備えたことを特徴とする。

【手続補正１０】
【補正対象書類名】明細書
【補正対象項目名】００１５
【補正方法】変更
【補正内容】
【００１５】また本発明は、ネットワーク経由で、他の計算機に対して電子化データを送付するデータ送付方法であって、前記電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記他の計算機に送付するステップと、前記他の計算機から前記圧縮データを受信した旨の通知を受けて、前記電子化データを前記他の計算機に送付するステップとを備えたことを特徴とする。

【手続補正１１】
【補正対象書類名】明細書
【補正対象項目名】００１６
【補正方法】変更
【補正内容】
【００１６】また本発明は、ネットワークで接続された第１、第２、第３の計算機を有し、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付システムであって、前記第１の計算機は、前記第３の計算機に対して認証を依頼する手段を備え、前記第３の計算機は、前記第１の計算機からの認証依頼に応じて認証を行う手段と、当該認証の結果に応じて、認証済みである旨の証明書データを作成し、前記第１の計算機に送付する手段とを備え、前記第１の計算機は、前記第３の計算機からの証明書データを受けて、電子化データに前記証明書データを付して証明書付きデータとし、前記第２の計算機に送付する手段を備え、前記第２の計算機は、前記第１の計算機からの証明書付きデータを受けて、証明書データが未使用のものであることを確認し、当該証明書付きデータを保管する手段を備えたことを特徴とする。また本発明は、第１、第２の計算機が接続されたネットワークを利用して、前記第１の計算機へ電子化データを送付するデータ送付装置であって、前記第２の計算機に対して認証を依頼する手段と、前記第２の計算機から認証結果を受けとる手段と、前記第１の計算機に送付する電子化データに前記認証結果を付した認証付きデータを作成する手段と、当該認証付きデータを前記第１の計算機に送付する手段とを備えたことを特徴とする。また本発明は、ネットワーク経由で、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付システムであって、前記第１の計算機は、電子化データを圧縮した圧縮データを作成する手段と、当該圧縮データを前記第２の計算機に送付する手段と、前記電子化データを前記第２の計算機に送付する手段とを備え、前記第２の計算機は、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較する手段とを備えたことを特徴とする。また本発明は、ネットワーク経由で、他の計算機に対して電子化データを送付するデータ

送付装置であって、前記電子化データを圧縮した圧縮データを作成する手段と、当該圧縮データを前記他の計算機に送付する手段と、前記他の計算機から前記圧縮データを受信した旨の通知を受けて、前記電子化データの前記他の計算機への送付を実行する手段とを備えたことを特徴とする。また本発明は、第１の計算機から第２の計算機に対して電子化データを送付するデータ送付方法を実現するプログラムを格納した記録媒体であって、前記データ送付方法は以下を含むことを特徴とする：前記第１の計算機で、電子化データを圧縮した圧縮データを作成し、当該圧縮データを前記第２の計算機に送付するステップと、前記電子化データを前記第２の計算機に送付するステップと、前記第２の計算機で、前記電子化データを受信後、当該電子化データと前記圧縮データとを比較するステップ。